PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-224461

(43)Date of publication of application: 17.08.1999

(51)Int.CI. G11B 20/10 G09C 1/00

(21)Application number : 10-025310 (71)Applicant : SONY CORP (22)Date of filing: 06.02.1998

(72)Inventor: ASANO TOMOYUKI OSAWA YOSHITOMO HASHIMOTO MEGUMI

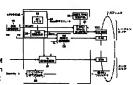
(54) INFORMATION PROCESSOR, INFORMATION METHOD, PROVIDING MEDIUM AND RECORDING MEDIUM

HO4L 9/32

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain intrincic information in a recording medium by decoding the intrincic information in the recording medium which are read out from the medium and are ciphered with an M. series code

SOLUTION: At first, a disk ID encryption decoding circuit 21 receives an EDiscID which is read out from the read-in area of an optical disk 7 and which is an ciphered DiscID. Next, the circuit 21 generates an EDiscID by decoding the EDiscID based on the predetermined M series code which is supplied from an M series code generating circuit 22 to output it to the hash function circuit 25 of an effective master key generating module 23. Moreover, M series codes to be supplied from the circuit 22 are codes which are given when proper licences are granted from copyright holders.



LEGAL STATUS

[Date of request for examination]

Date of sanding the examiner's decision of

rejection

[Kind of final disposal of a plication other than the examiner's decision of rejection or application converte registration

Date of final disposal for application

[Patent number]

Date of Agistration

[Number of app al against xam

of rej ction]

01/108/843

(19) 日本国特許庁 (JP)

(12) 公開特許公報(A)

(11)特許出顧公開番号 特開平11-224461

(43)公開日 平成11年(1999)8月17日

(51) Int.Cl.4	識別配号	FΙ	
G11B 20/10		G11B 20/10	н
G 0 9 C 1/00	660	G 0 9 C 1/00	660D
H 0 4 L 9/32		H04L 9/00	673E

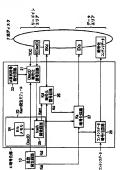
審査請求 未請求 請求項の数9 OL (全 11 頁)

(21)出願番号	特顯平 10-25310	(71)出職人	000002185	
			ソニー株式会社	
(22)出職日	平成10年(1998) 2月6日		東京都品川区北品川6丁目7番35号	
		(72)発明者	浅野 智之	
			東京都品川区北品川6丁目7番35号	ソニ
			一株式会社内	
		(72)発明者	大澤 裁知	
			東京都品川区北品川 6 丁目 7 番35号 一株式会社内	ソニ
		(72)発明者	横本 恵	
			東京都品川区北品川6丁目7番35号	ソニ
			一株式会社内	
		(74)代理人	弁理士 福本 義雄	

(54) 【発明の名称】 情報処理装置、情報処理方法、提供媒体、および記録媒体 (57) 【率約】

【課題】 記録媒体から読み出された暗号化された記録 媒体の固有情報をM系列符号で復号し、記録媒体の固有 情報を得る。

「解除手段」 ステップ531において、DiscD即等分化 係分回第21は、光ディスタ、のリードインエリアから 読み出された、暗号化されたDiscDであるEDiscDを受 け取る。DiscD即等分化度等回路21はさらに、ステップ 532において、M系列称号に基づいて、EDiscDを使 与して、DiscDを生成し、Kee発生モジュール23のhas 加製回路25に出力する。M系列称号時間22が検索 するM系列符号は、著作権者から適正なティセンスを受 けるときに、サストもれたものである。



【特許請求の範囲】...

の情報処理装置。

【精水項1】 着脱可能な記錄媒体に情報を記録または 再生する情報処理装置において

第1の秘密キーを発生する発生手段と、

前記記録媒体からそこに記録されている暗号化された前 記記録媒体の固有情報を受信する受信手段と、

前記発生手段により発生された第1の秘密キーにより、 前記受信手段により受信した暗号化された前記記数謀体 の固有情報を後号し、前記記数謀体の固有情報を生成す 名生成手段とを備えることを特徴とする情報処理装置 「請求項2」 前記記数媒体から暗号化された前記記録 媒体の固有情報を受信できないとき、乱数を発生する乱

数発生手段と、 前記第1の秘密キーにより、前記乱数を前記記録媒体の 固有情報として暗号化し、前記記録媒体に記録する記録 手段とをさらに備えることを特徴とする請求項1に記載

【請求項3】 前記生成手段により生成された前記記録 媒体の固有情報と、第2の秘密キーに基づいて、第3の 秘密キーを算出する算出手段と、

前記算出手段により算出された前記第3の秘密キーに対 応して、所定の情報を暗号化し、前記記録媒体に記録す る記録手段とをさらに備えることを特徴とする請求項1 に記録の情報処期診暦。

【請求項4】 前記所定の情報は、前記記録媒体に固有 の秘密キーであることを特徴とする請求項3に記載の情 類処理技術。

【請求項5】 前配第3の秘密キーにより、前記記録媒体から再生された前記記録媒体に固有の暗号化されている第4の秘密キーを復号する復号手段をさらに備え、

前記記録手段に、復号された前記第4の秘密キーを利用 して、所定の情報を暗号化し、前記記録媒体に記録する ことを特徴とする請求項3に記載の情報処理装置。

【請求項6】 前記第3の秘密キーにより、前記記録媒体から再生された前記記録媒体に固有の暗号化されている第4の秘密キーを復号する第1の復号手段と、

復号された前記第4の秘密キーを利用して、前記記録媒体から供給された時号化されているデータを復号する第 2の復号手段とをさらに備えることを特徴とする請求項 3に記載に情報処理装置。

【請求項7】 着脱可能な配鉄媒体に情報を記録または 再生する情報処理装置の情報処理方法において、 第1の秘密キーを発生する発生ステップと

前配配録媒体からそこに記録されている暗号化された前 記記録媒体の固有情報を受信する受信ステップと、

前配発生ステップにより発生された第1の秘密キーにより、前記受信ステップにより受信した時号化された前記 記録媒体の固有情報を復号し、前記記録媒体の固有情報 を生成する生成ステップとを備えることを特徴とする情報 報処理方法。 【請求項8】 着脱可能な記録媒体に情報を記録または 再生する情報処理装置に使用するコンピュータプログラ ムであって

第1の秘密キーを発生する発生ステップと、

前記記録媒体からそこに記録されている暗号化された前 記記録媒体の固有情報を受信する受信ステップと、

前記発生ステップにより発生された第1の秘密キーにより、前記受信ステップにより受信した暗号化された前記 記録媒体の固有情報を復号し、前記記録媒体の固有情報 を生成する生成ステップとを備えるコンピュータプログ ラムを提供することを特徴とする提供媒体。

【請求項9】 情報処理装置に装着され、情報が記録または再生される記録媒体において、

M系列符号で暗号化した前記配録媒体に固有の情報が記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

[0001]

【発明の属する技術分野】本発明は、情報処理装置、情報処理方法、提供媒体、および記録媒体に関し、特に、より安全にデータを授受することを可能にする情報処理装置、情報処理方法、提供媒体、および記録媒体に関する。

[0002]

【従来の技術】近年、情報をデジタル的に記録する記録 機勝および記録媒体が普及しつつある。これらの記録機 認および記録媒体が普及しつつある。これらの記録機 認および記録媒体が再発し、再生するので、データを、そ の質を維持しながら何度もコピーすることができる。 いしながら、後後や音楽のブータの著作権等にしてみれ ば、自らが著作権を有するデータが、その質を維持しな いら何度も下正にコピーされ、市場に流通してしまう恐 れがある。このため、記録機器および記録媒体の何で、 著作権を有するデータが不正にコピーされるのを防ぐ必 要がある。

戻りのの。 [0 0 0 3] 例えば、ミニディスク (MD) (商標) シス テムにおいては、SOMS(Serial CopyManageaent System) と呼ばれる方法が用いられている。これは、デジクルイ ンタフェースによって、音楽データとともに伝送される 情報のことである。この情報は、音楽データが、copy f ree、copy once allowed、まだはcopy prohibitedのう ちのいずれのデータであるのかを表す。ミニディスクレ コーダは、デジクルインクフェースから音楽データを受 信した場合、SOMSを検出し、これが、copy prohibited であれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedで要更 し、受信した音楽データとともに記録し、copy freeで あれば、これをそのまま、受信した音楽データとともに

【0004】このようにして、ミニディスクシステムに おいては、SOMSを用いて、著作権を有するデータが不正 にコピーされるのを防いでいる。

【0005】また、著作権を有するデータが不正にコピ でされるのを砂で別の例としては、Digital Versatile Disk(DVD) (商標) システムにおける、コンテンツスタ ランブルシステムがあげられる。このシステムでは、デ ススタ上の、各権権を有するデータが全で報号化され、 ライセンスを受けた配換機器だけが暗号線を与えられ、 これにより略号化されたデータ後等し、意味のあるデータを得ることができるようになされている。そして、 配験機器は、ライセンスを受ける際に、不正コピーを行 わない等の動件規定に従うように設計される。このよう にして、DVDシステムにおいては、著作権を有するデータが不正にコピーされるのを助いている。

[0006]

【発明が解決しようとする課題】しかしながら、上記の ミニディスクシステムが採用している方式では、SOMSが copy once allowedであれば、これをcopy prohibitedに 変更し、受信したデータとともに記録するなどの動作規 定に従わない記録機器が、不正に製造されてしまう。

[0007]また、上記のDVDシステムが採用している 力式は、ROMメディアに対しては有効であるが、ユーザ がデータを記録可能なRAMメディアにおいては有効では ない。RMメディアにおいては、不正管は、暗号を解談 等しいディスクに不正にコピーすることによって、ライ センスを受けた正当な記録機能で動作するディスクを新 たに作ることができるからである。

【0008】本発明はこのような状況に鑑みてなされた ものであり、例えば、著作権者から適正に利用許可を受 けた者にだけ与えられる秘密キーに基づいて、記録媒体 に固有の情報にアクセスできるようにすることで、不正 コピーを防止するものである。

[0009]

【課題を解決するための手段】請求項1 に記載の情報処理装置は、第1の秘密オーを発生する発生手段と、記録はなからそこに記録されている時号ともれた既健体の固有情報を受信する受信手段と、発生手段により発生された第1の秘密キーにより、受信手段により受信した時代とれた記録体の固有情報を復りし、記録体の固有情報を生成することを特徴とす

【0010】請求項7に記載の情報処理方法は、第1の 秘密キーを発生する発生ステップと、記録媒体からそこ に記録されている時号化された記録媒体の超情報を受 情する受情ステップと、発生ステップにより発生された 新1の秘密キーにより、受情ステップにより受信した時 号化された記録媒体の固有可報を復分し、記録媒体の固 有情報を追成する生成ステップとを個えることを特徴と する情報処理方法。

【0011】請求項8に記載の提供媒体は、第1の秘密

キーを発生する発生ステップと、配録媒体からそこに配 数されている暗号化された記録媒体の固有情報を受信す の受信ステップと、発生ステップにより発生された第1 の秘密キーにより、受信ステップにより受信した暗号化 された記録媒体の固有情報を包号し、記録媒体の固有情報を 数を生成せる生成ステップとを備えるコンピュータブロ グラムを提供することを特徴とする。

【0012】請求項9に記載の記録媒体は、M系列符号 で暗号化した記録媒体に固有の情報が記録されているこ とを特徴とする。

[0013] 請求項1に記載の情報処理装置、請求項7 に記載の情報処理方法、および請求項8に記載の情報処理 体においては、第1の秘密キーが発生され、記録媒体か らそこに記録されている時号化された記録媒体の固有情報が受信され、発生された第1の秘密キーにより、受信 した時号化された記録媒体の固有情報が復号され、記録 媒体の固有情報が進安され、記録 媒体の固有情報が進安され、記録 媒体の固有情報が進安され、記録

[0014]

【発明の実施の形態】以下に本規則の実施の形態を説明 うるが、特許様々の範囲に登録の発明の多手段と以下の 実施の形態との対応関係を明らかにするために、各手段 の後の搭弧内に、対応する実施の形態(但し一例)を付 加して本発明の特徴を記述さると、次のようになる。 但 し勿論この記載は、各手段を記載したものに限定するこ をを意味するものではない。

[0015] 請求項1に記載の情報処理装置は、第1の 秘密キー (子め定められた以来列符号)を発生する発生 手段(例えば、図3のM系列符号発生回路2)と、記 録媒体からそこに記録されている時号化された記録媒体 の固有情報(回1scID)を受信する受信手段(例えば、 図3の助iscID呻号化復号回路21)と、発生年段により 発生された第1の秘密キーにより、受信手段により受信 た時呼化された記録媒体の固有情報を復号、記録媒 体の固有情報(01scID)を生成する生成手段(例えば、 図3の助iscID呻号化復号回路21)とを備えることを特 後とする。

【0016] 請求項2に起軟の情報処理装置は、記録紙 体から時号化された記録紙や固有情報を受けっさない とき、乱散を発生する乱散発生手段(例えば、図3の乱 鉄線性の固有付権とあて時年により、乱散を記 級域体の固有付権として時号化し、記録は形に記録する 記録手段(例えば、図3の助iscD時号化度号回路21) とをさらに優えることを特度とする。

[0017] 請求項3に記載の情報処理装置は、生成手 砂により生成された記録様本の副有情報と、第2の秘密 キー (マスタネーKa)に基づいて、第3の秘密キー (イ フェクディグマスタキーKea) を裏出する第1年度 式ば、図3のbash限数回路25)と、第11年形により算 出された第3の秘密キーに対応して、所定の情報を錯号 化し、記録様性に記録する配象手段 (例えば、図3のKd 暗号化復号回路26)とをさらに備えることを特徴とする。

【0018】請求項5に記載の情報処理装置は、第3の 慰密キーにより、記録媒体から再生された記録媒体に関 有の暗号化されている第4の秘密キー(暗号化ディスク キー区40 を復号する復号手段(例えば、図3の以1錯号 化復号回路26) をさらに備え、記録手段に、復号され た第4の秘密キー(マスクキーKd)を利用して、所定の 情報を暗号化し、記録媒体に記録することを特徴とす ス・

[0019] 請求項6に記載の情報処理装置は、第3の 宿の時寺化とれている第4の税金キーを複サする第1の 復号手段(例えば、図4の既は復号回路56)と、復号 された第4の報告十を利用して、記録媒体から供給さ れた第4の記録キーを利用して、記録媒体から供給さ れた第50歳年十を利用して、記録媒体から供給さ れた第5化されているデータを復号する第2の復号手段 (例えば、図4の区域野分化回路57およびコンテンツ デーク度等中図858)とををさらに備えることを特徴とす

[0020] 図1は、本処明を適用した光ディスク記録 再生装置の構改例を表している。入力部11は、ボタン、 スイッチ、リモートコントローラなどにより構成され、 ユーザにより入力操作されたとき、その入力操作に対応 する信号を出力する。削御回路をは、記憶されている所 定のコンピュータブログラムに従って、装置全体を制御 する。

[0021] 記録再生回路3は、時号化路4と復号路7 を有し、復号部5は、ビックアップ6により、光光7ス クアから再生されたデータを復号し、外部に再生信号と して出力する。暗号化部4は、外部から記録信号の供給 を受け取ると、これを暗号化し、ビックアップ6に供給 して、光ディスク7に記録させる。

【0022】ピックアップ6は、レーザピームを光ディスク7に照射することで、データの記録再生を行う。ス

ここでマスタキーMaiは、著作権者等から適正にライセンスを受けた者(光ディスク配録再生装置)にだけ与えられる秘密のキーである。また、ここで、例えば、AとBの結合とは、それぞれが32ピットであるとき、Aの後方にBを結合して、64ピットのデータとすることを意味する。

[0027] 光ディスクィのデータエリアの各セクタ5: (i=1,2,...)は、ヘッダおよびメインデータ節で構成され、ヘッダには、セクタキーKsiをディスクキーKdで精 号化した暗号化セクタキーEKsi(i=1,2,...)が格納されている(ここでKsiのiは、セクタの番号を示し、セクタキーはセクタ毎に異なるのでKsiと記述する)。メインデータ節には、コンテンツデータをセクタキーKsiで暗号化した暗号化コンテンツデータをセクタキーKsiで暗号化した暗号化コンテンツデータをセクタキーKsiで暗号化した暗号化コンテンツデータをセクタキーKsiで暗号化した暗号化コンテンツデータをセクタキーKsiで暗号

ピンドルモータ9は、サーボ回路8によって制御され、 光ディスク7を回転させる。

【0023】サーボ回路8は、スピンドルモータ9を駆 動することにより、光ディスク7を所定の速度で(例え ば線速度一定で)回転させる。サーボ回路8はまた、ピ ックアップ 6 のトラッキングおよびフォーカシングの 他、スレッドサーボを制御する。乱数発生回路10は、 制御回路2の制御により、所定の乱数を発生する。 【0024】光ディスク7には、図2に示すような構造 を有するデータが記録されている。光ディスク7のリー ドインエリアには、光ディスクのID (以下、DiscIDと称 する)を予め定められたM系列符号で暗号化したEDiscI D、デイスクキーKdをイフェクティブマスタキーKemで暗 号化した暗号化ディスクキーEKdが記録されている。 【0025】M系列符号は、所定の周期で、"0"と" 1"の2値がランダムに出現する疑似ランダム2値信号 (一種の疑似乱数) であり、DiscIDは、例えば、ファイ ル名やデイレクトリ情報などのTOC(Table Of Contents) データ内に、予め設定された所定のM系列符号に基づい て埋め込むことで暗号化されている。すなわち、DiscID は、TOCデータのエッジの時間ずれとして記録される。 このような暗号化を行うと、TOCデータはM系列符号が なくとも読み取ることができるが(TOCデータは暗号化 されないが)、DiscIDはM系列符号がないと読み取る (復号する) ことができなくなる。このようなM系列符 号に基づく暗号化に関する技術は、特願平09-288960号 として本出願人が先に提案している。なお、この所定の

際、後述するマスタキーKmとともに、ライセンスを受け た者に与えられる。 【0026】イフェクティブマスタキーKeeiは、式 (1)に従い、マスタキーKmとDiscIDの結合にhash開数 を適用して計算される。

M系列符号は、著作権者から適正なライセンスを受ける

イフェクティブマスタキーKem=hash (マスタキーKm+DiscID) (1)

【〇〇2名】図3は、時号化係4の構成例を楽している。 あ。DiscID時分化復号回路21は、光ディスク7から み、DiscID時分化復号回路21は、光ディスク7から 始されるM系列符号に基づいて復号し、DiscIDを生成分 あ。DiscID時で低号回路21はまた、乳炭を三路1 のから発生された乱敷をDiscIDとして受け取り、M系列 符号発生回路22から供給されるM系列符号に基づ て、上述したように、入力されるTOC情報に進め込むように暗号化して、EDIscIDを生成し、光ディスク7に記 後する。

[0029] M系列符号発生回路22は、例えば、直列接続された複数のフリップフロップとイクスクルーシブ オプ回路からなり、所定のM系列符号を発生するように なされている。あるいは、ROM、EEPROMなどで構成する こともできる。 【0030】 Kes発生モジュール23のKmメモリ24 は、マスタキーKmを記憶する。Kem発生モジュール23 のhash関数回路25は、マスタキーKmとDiscIDの結合を 生成し、これにhash関数を適用してイフェクティブマス タキーKemを質出する。

[0031] Ks時号化境号回路26は、光ディスク7か 応路み出された暗号化ディスタ+ 下Ktdを イフェッテ ィブマスタキー Ksdで で で けった ディスクキー Kdを生成 する。Kd時号化電号回路26はまた、私放発生回路10 から発生された気象をディスタ+ 下Kdとして暗号化ディ スタキーFKBを全成し、光ディスク7に影響オースクラー スタキーFKBを全成し、光ディスク7に影響オースクラー ディスタキーFKBを全成り、光ディスク7に影響オースクラー ディスタキーFKBを全成り、光ディスク7に影響オースクラー ディスター FKBを全成り、光ディスク7に影響オースクラー ディスター FKBを全成り、光ディスク7に影響オースクラー ディスター FKBを表現り、光ディスク7に影響オースク7に影響オースクラー ディスター FKBを表現り、光ディスク7に影響オースクラー ディスター FKBを表現り、光ディスク7に影響オースク7に影響オースクラー ディスター FKBを表現り、光ディスク7に影響オースクラー ディスター FKBを表現り、ディスク7に影響オースクラー ディスター FKBを表現り、ディスク7に影響オースクラー ディスター FKBを表現り、ディスクア FKBを表現り、ディスクラー ディスター FKBを表現り、ディスクラー ディスター FKBを表現り、ディスクラー ディスクラー ディスクー

【0032】Ks時号化回路27は、私数発生回路10から発生された私数をセクタキーKsとして受け取り、ディスクキーKitが軽々化て時代化化等化性とクタキーKsを生成し、光ディスク7に配除する。コンテンツデータ時号化回路28は、セクタキーKsで、コンテンツデータを暗号化し、光ディスク7に配除する。

【0033】 吹に、図4に、復号部5の構成例を示す。 EDiscl版は号回路51は、光デイスタ7から読み出され たEDisclDを、M系列符号発生回路52から供給される M系列符号法基づいて復参して、DisclDを生成する。M 系列符号発生回路52は、M系列符号配路22と同様の 構成を有し、M系列符号発生回路22と同一のM系列符号を発生するようになされている。

【0034】Kem発生モジュール53のKmメモリ54 は、マスタキーKmを配施する。Kem発生モジュール53 のhash開教回路55は、マスタキーKmとDiscIDの結合を 生成し、これにhash開教を適用してイフェクティブマス タキーKemを計算する。このKem発生モジュール53は、 Kem発生モジュール23と同一の構成とされ、両者を兼 用するようにしてもよい。

【0035】EXd復争回路56は、光ディスク7から読み出された培号化ディスクキーEXdを、イフェクティア

マスタキーKerrで復号して、ディスタキーKdを はつまった。

5. EXS復号回路57は、光ディスク7から各セクタSiのヘッグに記録されている培引化セクタキーEXSを読み

出し、ディスタキーKerを質して、セクタキーKeを算出する。
コンテンツデータ復号回路58は、光ディスク7から読み出された培号化されたコンテンツデータを、セクタキーKrで優号する。

【0036】次に、ユーザデータが光デイスク7に配験される場合の時号化部4とおける処理手順を、図5のフローチャートを参照して説明する。なお、この例の場合のは、光ディスク7製造時に、光ディスク7に書き込まれているものとする。

【0037】最初に、ステップS31において、DiscID 時号化復号回路21は、光ディスク7のリードインエリ アから読み出された、暗号化されているDiscIDであるED iscIDを受け取る。DiscID時号化復号回路21はさら に、ステップS32において、M系列符号発生回路22 から供給された所定のM系列符号に基づいて、EDisciD を復与して、DisciDを生成し、Kem発生やジュール23 のhash関数回路25に出力する。M系列符号回路22が 供給するM系列符号は、著件維密から適正なタイセンス を受けるときに、与えられたものである。

【0038】ステップS33において、Kem発生モジュール23のhash関数回路25は、Kem発生モジュール23のhash関数回路25は、Kem発生モジュール23のhash関数回路25はさらに、ステップS34で、上述の式(1)に従い、光ディスク7のDisclDとマスクキーKamの結合にhash関数を適用して、イフェクティブマスクキーKamの結合にhash関数を適用して、イフェクティブマスクキーKamの結合にhash関数を適用して、イフェクティブマスクキーKamの結合にある対象が表現を通用して、イフェクティブマスクキーKamの計算と、Kdr時号化復号回路26に接続する。

【0039】 於に、ステップS35において、Kd暗号化 復号回路26は、光ディスク7のリードインエリアから 該み出された暗号化ディスクチーEXはを受け取る、Kdm 号化復号回路26は、ステップS36で、光ディスク7 のリードインエリアに、暗号化ディスクキーEXはか書き 込まれているか否か(暗号化ディスクキーEXはを受け取 ることができたか否か)の判定を行う。暗号化ディスク 十二既はが書き込まれていないと判定された場合、ステ ップS37に進み、乱散発生回路10は、40ピットの 乱散を発生し、ディスクキーKはとして、Kd暗号化復号回 826に出力する。

【0040】次に、ステップS38において、Kam時分化 復号回路26は、乱数発生回路10から供給されたディ スクキーKde、Lash開放回路55から受け取ったイフェ クティブマスタキーKenlcより暗号化して、暗号化ディ スクキーEKdを生成し、光ディスタ7のリードインエリ アに記録する。

100411ステップS36で、暗号化ディスクキー医 が審き込まれていると判定された場合、ステップS3 9に過み、Kd時号化復号回路26は、この光ディスク7 から設み出された暗号化ディスクキーEKdを、kash開設 回路25から受け取ったイフェクティプマスタキーKen で復号して、ディスクキーKdを得る。Kd暗号化復号回路 26は、そのディスクキーKdを、Ks暗号化回路27に出 カする。

【0042】ステップS38またはS39の地理の後、乱聚発生回路10は、ステップS40で、40ビットの 乱敷を発生し、セクタキー私として、Ks時代回路27、およびコンテンツデータ時号化回路28に出力する、Ks時号化回路27は、ステップS41で、Ks時号化回路266時間を27は、ステップS41で、Ks時号化回路266時間を27は大力スク下に記録されている場合)、または乱散発生回路10時代ディスクイに記録されていない場合)から受け取ったディスクキーKstで、乱散発生回路10から受け取ったディスクキーKstで、乱散発生回路10から受け取ったナイスクキーKstで、乱散発生回路10から受け取ったナイスクキーKstで、乱散発生回路10から受け取ったナクタキーKsを時号化して、時号

た、その暗号化セクタキーEKsを、光ディスク 7のデー タエリアにあるセクタヘッダに記録する。

【0043】次に、ステップS42において、コンテン ツデータ暗号化回路28は、(ステップS40で乱数発 生回路10から受け取った)セクタキーKsにより、コン テンツデータを暗号化し、光ディスク7のデータエリア のメインデータ部に記載する。

【0044】ステップS43において、時号化前4の各 直を行う。全てのコンテンツデータを記録したか否かの判 定を行う。全てのコンテンツデータがまた記録されてい ないと判定された場合、ステップ44に進み、暗号化節 4の各回路は、光ディスク7の、まだデータを記録してい ないセクタにアクセスし、ステップS40に戻り、以 下同様の批理を繰り返す、ステップS40で、全てのコ ンテンツデータが記録されたと判定された場合、暗号化 部4の各回路は、全ての記録处理を終すする。

【0045】以上のようにして、著作権者から適正なラ イセンスを受けるときに、与えられた所定のM系列符 で、暗号化されたDiscIDを復号し、DiscIDを得ることに より、暗号化した情報が記録媒体に記録される。

【0046】次に、製造時に、DiscIDが記録されていな い光ディスク7に対して、ユーザデータを記録する場合 の暗号化部4における処理手順を、図6のフローチャー トを参照して説明する。

【0047】最初に、ステップS51において、DiscID 時号化復号回路21は、光ディスクアのリードインエリ アから読み出されたEDiscIDを受け取り、またK4時号化 復号回路26は、光ディスクアのリードインエリアから 読み出された時号化ディスクキーEKdを受け取る。

【0048】 次に、ステップS52において、Disc1D時 今化復号回路21は、光ディスクスのリードインエリア に、即isc1Dが書き込まれているか否か(即isc1Dを受け ることができたか否か)の判定を行い、KM時等化復号回 第26は、光ディスクスのリードインエリアに、時号化 ディスクキーEKはが要き込まれているか否か(時号化デ ィスクキーEKはを受け取ることができたか否か)の判定 を行う。即isc1Dを時予化ディスクキーEKは対策に書き込 まれていないと判定された場合、ステップS53に進 み、思数を足回路10年10年2日と日とリーの記載を発生 し、Disc1Dとして、Disc1D時号化復号回路21に出力す

[0049] 於に、ステップ554において、DiscID時 号化復号回路21は、乱聚発生回路10から供給された 別5sIDを、M系列符号発生回路22から供給されたM系 列符号に基づいて、上途したように、TOC情報中に埋め 込むようにして暗号化して、EDiscIDを生成し、光ディ スク7のリードインエリアに記載する。

【0050】次に、ステップS55において、Kem発生 モジュール23のhash関数回路25は、Kem発生モジュ ール23のKmメモリ24から、マスタキーKmを読み出 す。Kes陽生モジュール23のhash開数回路25は、ステップS56で、上途の式(1)に従い、光ディスク7のDiscID、およびKmメモリ24から読み出したマスタキーKmの結合にhash開数を適用して、イフェクティブマスタキーKenを計算し、Kd晴号化復号回路26に供給する。

【0051】 次に、ステップS57において、乱散発生 回路10は、40ピットの乱散を発生し、ディスクキー などして、た明号化復号回路26に出力する。応時号化 復号回路26は、ステップS58において、乱散発生回 810から使わるため、ステップS58において、乱散発生の 810から使わるたがディスタキーKed・Lashに限数回路 25から受け取ったイフ=クティブマスタキーKedによ り時号化して、暗号化ディスクキーERGを生成し、光ディスクィのリ・ドインエリアに記録する。

【0052】ステップS52で、EDiscIDと暗号化ディスクキーERAが書き込まれていると判定された場合、ステップS5に進み、DiscID等や化復号回路21は、この光ディスクから読み出されたEDiscIDを、M系列符号回路22から使給されたM系列符号で復号して、DiscIDを生成する。

【0053】 ステップ S60において、Kee発生モジュール23のhash関数回路25は、Kee発生モジュール23のhash関数回路25は、Kee発生モジュール23のhash関数回路25は、ステップ S61で、上途の数(1)に使い、光ディスタ Toplisc IDとマスタキーKamの結合にhash関数を適用して、イフェクティブマスタキーKamの結合にhash関数を適用して、イフェクティブマスタキーKamの結合にhash関数を適用して、イフェクに供給する。

【0054】次に、ステップ562において、Ku時号化 億分回路26は、この光ディスクイから渡み出された時 号化ディスクキーEKdを、hash開教回路25から受け取 ったイフェクティブマスクキーKemで復号して、ディス クキーKdを得る。Kd時号化復号回路26は、ディスクキ ーKdを、Ks時号化回路27に出力する。

【0055】ステップS58またはS62の処理の後 は、ステップS63に進むが、ステップS63万至S6 7で行われる処理は、図50ステップS40万至S4 で行われる処理と関係の処理であり、全てのコンテンツ データが記録された当党された場合、全ての配録処理 が終すする。

[0056]以上のようにして、DiscIDが生成され、配 数媒体に記録され、そして生成されたDiscIDとマスタキ 一版に対応して暗号化されたコンテンツデークが記録媒 体に記録される。このことより、例えば、既存の記録媒 体(DiscIDが記録されていない思媒体)に記録されて コンテンツデータを、著作権者から違正にライセンスを 受けていない者は、意味のある情報として再生すること ができない。

【0057】次に、図7のフローチャートを参照して、 復号部5により行われる、ユーザデータの再生処理を説 明する。最初に、ステップS 81 において、EDiscIDで み出された、暗号化されたDiscIDであるEDiscIDを受け 取る。EDiscIDを号間係51 はさらに、ステップS 82 において、MR列符号発生回路52 から供給されたM系 利符号に基づいて、EDiscIDを優号してDiscIDを生成 し、Kee発生モジュール53 のhash開数回路55に出力 する。

【0058】次に、ステップS83において、Kem発生 モジュール53のhash開放回路55は、EDiscIDを号回 筋51から出力されたDiscIDを受け取るとともに、Kmメ モリ54からマスタキー転を読み出し、上述の式(1) に従い、光ディスタ7のDiscIDセマスタキーKemを結 hash開設を適用してイフェクティブマスタキーKemを算 出し、EKG低号回路56に供給する。

【0059】ステップS84において、胚/復号回路ら 6は、光ディスクのリードインエリアから総を出された暗号化ディスクキーEKdを受け取る。EKd復号回路ら は、ステップS85で、この読み出された暗号化ディス ノキーEM&を、hasiの数を開きらちから受け取ったイフェ クティブマスクキーKacで復号して、ディスクキーKdを 算出し、EKG復行回路ら7に出力する。

【0060】次に、ステップ 886において、ENS護母 回路57は、光ディスク10mデータエリアから読み出さ れた各セクタの暗号化セクタキーENsi(に=1,2,...)を 受け取る。ENS護母回路57は、ステップ S87で、こ の読み出された時号化セクタキーENsiを、EXI復号回路 56から受け取ったディスクキーKaで復号して、セクタ キーKsiを算出し、コンテンツデータ電号回路58に出 力する。

[006.1] ステップ S8 Bにおいて、コンテンツデー 夕俊号回廊 S8 は、光ディスク 7から読み出された暗号 化されているコンテンツデータを受け取る。コンテンツ データ 優知回路 58 は、ステップ S8 9で、この読み出 自れた暗号化とれているコンテンツデータを、既確号 回路 57 から受け取ったセクタキーKsiで復号し、再生 信号として出わする。

【0062】 次に、ステップ S90において、復今部5 の各回路は、光ディスク1のデータエリアから、全ての コンテンツデータを読み出したか否かの判定を行う。全 てのコンテンツデータがまた読み出されていないと判定 された場合、ステップ S91に进み、復号部5の各回路 は、光ディスク1の、まだ読み出されていない次のセク タのデータの供給を受け、ステップ S86以所の処理を 繰り返す。全てのコンテンツデータが読み出されたと判 走された場合、復号部5の各回路は、全ての再生処理を 終了する。

【0063】このように、記録媒体のIDを生成し、所定 のM系列符号で暗号化して、記録媒体に記録すること で、著作権者から適正にライセンスを受けた者だけが、 その記録媒体にアクセスできるようにする。

[0064]本発明は、光ディスク以外の世野媒体にデータを記録まは同率する場合にも適用が可能である。
[0065]なお、本明細書中において、上記処理を実行するコンピュータブログルをユードに発性する提供様体には、磁気ディスク、CD-Roukをどの情報を登録体の他、インターネット、デジタル衛星などのネットワークによる伝送接件も含まれる。

[0066]

【発明の効果】請求項1と記載の情報処理接臘、請求項 「に認敬の情報処理方法、および請求項8に勤助の提供 媒体によれば、第1の秘密ホーにより、配録媒体に記録 されている母子化された記録媒体の固有情報を復与し、 比数媒体の回角情報を生成するうにしたので、例え ば、予め定められた州系列符号を有していない者が、記 解媒体にアクモスオることを相談にする。

[0067] 請求項とに定数の情報処理装置によれば、 記数媒体の占有等サイビされた影響体の固有情報として暗号化 し、記数体に記録するようにしたので、例えば、予め 定められた処式が再分を有していない者は、記録媒体の 固有情報が記録されていないをは、記録媒体の 固有情報が記録されていない記録媒体に記録されている 情報を、発生することができない。

【0068】 請求項3に記載の情報処理装配とよれば、 生成手段により生成された記録体の国有情報と、第2 の秘密キーに基づいて、第3の秘密キーを算出し、算出 された第5の秘密キーに対応して、所定の情報を暗号化 、記録媒体に記録するようにしたので、予め定められ たM系列科号を有していない者が、記録媒体にアクセス することを、さらに困難にする

【0069】請求項9に記載の記録媒体によれば、M系 列符号で暗号化した記録媒体に因有の情報を記録するよ うにしたので、情報処理装置に記録媒体の固有情報を提 供することができる。

【図面の簡単な説明】

【図1】本発明を適用した光ディスク記録再生装置の一 実施の形態の構成を示すプロック図である。
【図2】光ディスクに記録されるデータを説明する図で

ある。 【図3】図1の暗身化部4の内部の構成を示す図であ

図3】図1の暗号化部4の内部の構成を示す図であ

【図4】図1の復号部5の内部の構成を示す図である。
【図5】図1の暗号化部4の動作を説明するフローチャートである。

【図6】図1の暗号化部4の他の動作を説明するフローチャートである。

【図7】図1の復号部5の動作を説明するフローチャートである。

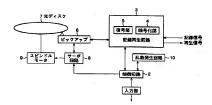
【符号の説明】

1 入力部、2 制御回路、3 記録再生回路、4 暗

. 号化師, 5 復号部, 6 ピックアップ, 7 光ディスク, 8 サーボ回路, 9 スピンドルモータ, 10 私 数発生回路, 2 1 Discl即号では場合回路, 2 2 M系 列符号発生回路, 2 3 Ken発生モジュール, 2 4 Ka メモリ, 2 5 hash関数回路, 2 6 Kd軒号化復号回

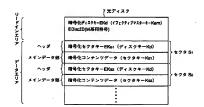
路, 27 Ks時号化回路, 28 コンテンツデータ暗号 化回路, 51 EDiscID復号回路, 52 M系列符号発 生回路, 53 Kee発生モジュール, 54 Kmメモリ, 55 hash開数回路, 56 EKd復号回路, 57 EKs復 号回路, 58 コンテンツデータ復号回路

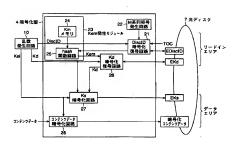
[図1]



光ディスク記録再生装置

[図2]





【図4】

